UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG, INC.,

Plaintiff,

v.

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50.

Defendants.

Civil Action No. 1:22-cv-00187-LJV-JJM

DEFENDANT SKYRYSE, INC.'S MOTION FOR AN ORDER ADOPTING FORENSIC PROTOCOL

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

RULES

I. INTRODUCTION

Defendant Skyryse does not want, does not need, and never intended to obtain any alleged trade secret information from Plaintiff Moog. Skyryse has gone to great measures to identify anything in its company that Moog has vaguely alleged to be its trade secret information, ensure it is not being used, and deliver it to Moog. To that end, Skyryse stipulated to a March 11 Order largely drafted by Moog (Dkt. Nos. 25, 28) that gave Moog the preliminary relief it claimed it needed, including the delivery of any alleged non-public Moog information to Moog. Skyryse takes these obligations seriously and has been working tirelessly with counsel and outside vendors to ensure compliance with the Stipulated Order.

The Stipulated Order recognizes that certain files that Moog claims include its trade secrets may be intertwined with Skyryse's own confidential information. In that event, it requires Skyryse to produce such information "to a third-party forensics firm mutually agreed upon by the parties … for forensic imaging *in lieu of providing such information directly to Plaintiff*."[1] (Dkt. No. 25, ¶ 2.) Moog proposed using the neutral forensics firm iDS for this purpose, and Skyryse agreed. To date, Skyryse has delivered to iDS a Skyryse-issued laptop computer used by Defendant Kim, two Skyryse-issued laptops used by Defendant Pilkington, an external hard drive with over 11,000 files found on another of Mr. Pilkington's laptops, and a hard drive containing two additional files from Skyryse's Gitlab source code repository. Defendants Kim and Pilkington separately have provided to iDS 23 additional devices. And Moog has argued that Skyryse should provide *dozens* of additional laptops to iDS. iDS thus has (or may have) in its possession forensic images—essentially replicas or mirror images—of *the contents of each device as a whole including files,*

[1] All emphasis in quotes has been added unless otherwise indicated.

source code, and applications, not just select files or data relevant to the claims and defenses in this action.

Under the Stipulated Order, the parties are to try to "agree on a protocol for searching all such information delivered to the Forensics Firm *for use in discovery*." (*Id.*, ¶ 3.) That they have been unable to agree brings us here. The core of this dispute is how to ensure that Moog can take fair, proportionate discovery of information on the devices in iDS's custody without embarking on an unreasonable, unbounded fishing expedition that would expose Skyryse's confidential, irrelevant information and unfairly prejudice Skyryse in this lawsuit. Moog's forensic protocol is not just unreasonable in its breadth and unprecedented, it also would give it the very sort of unfair tactical advantage that courts routinely warn about: allowing a plaintiff to pore over its adversary's (here, an alleged competitor's) most sensitive information before the plaintiff has sufficiently identified its own alleged trade secrets, so it can craft a litigation theory of misappropriation tailored to what it learns about its adversary's work with hindsight. This is exactly backwards.

Only Skyryse's proposed protocol strikes the right balance, consistent with precedents permitting forensic discovery while guarding against undue intrusiveness and unfairness. Skyryse's proposal would let Moog instruct iDS in detail, using thousands of search terms, to search the defendants' images for discoverable information; it would allow Skyryse to review any "hits" for privilege and responsiveness; and it would result in the production of non-privileged, responsive information to Moog.

Moog's proposal, by contrast, would defeat the purpose of a "third-party forensics firm." It would reduce iDS's role to an artifice and give Moog's lawyers and experts access to *all of the complete images* of the defendants' machines with no limitations as to scope, topic, or relevance. It would be as if Moog's lawyers and experts were handed the keys to Skyryse's offices and the

passwords to its computers, and allowed to rummage through millions of files with no restrictions. This would be unreasonable even if Moog had identified with sufficient particularity what its alleged trade secrets are. It does not matter at all that iDS would retain physical possession of the devices since their entire contents still would be exposed to Moog's counsel and experts. This is a classic fishing expedition and the Court should reject it, adopting Skyryse's proposal instead.

II. SKYRYSE'S PROPOSED PROTOCOL IS FAIR, BALANCED, AND CONSISTENT WITH PRECEDENT.

Skyryse's proposed forensic protocol (filed earlier with the Court at Dkt. No. 76-1 and included with this motion as Exhibit A) follows a structure endorsed by many courts that have ordered litigants to work with an independent neutral on forensic aspects of discovery: (1) the parties work out an appropriate set of search terms, (2) instruct a neutral forensic expert who has custody of the imaged computer systems to run searches across the imaged devices, (3) the producing party gets the opportunity to review the "hits" to address any privilege and responsiveness concerns, and (4) the non-privileged, responsive files are produced in discovery. *See, e.g., Wynmoor Cmty. Council, Inc. v. QBE Ins. Corp.*, 280 F.R.D. 681, 687–88 (S.D. Fla. 2012) (ordering a forensic expert to mirror computer systems; the parties to work with the court to determine search terms; the expert to search the images; and the resulting responsive documents to be produced after the producing party reviews them for privilege and responsiveness); *Sony BMG Music Ent. v. Arellanes*, No. 4:05-CV-328, 2006 WL 8201075, at *1 (E.D. Tex. Oct. 27, 2006) (ordering same); *Ameriwood Indus., Inc. v. Liberman*, No. 4:06CV524-DJS, 2006 WL 3825291, at *5 (E.D. Mo. Dec. 27, 2006) (ordering appointment of independent expert to image and recover all files from defendants' hard drives and provide them to defendants' counsel, with defendants to produce any non-privileged, responsive documents to plaintiff); *see also, e.g., Brocade Comm'ns Sys., Inc. v. A10 Networks, Inc.*, No. 10-CV-03428-LHK, 2012 WL 70428, at

*3 (N.D. Cal. Jan. 9, 2012) (ordering, in a case with trade secret and other IP claims, that if parties could not agree on using the plaintiff's forensic expert, to "select[] a neutral third party expert to conduct the inspection," and in all events requiring "the forensic expert produce any recovered files to [defendant] first, to all [defendant's] counsel to review the files as to relevance, responsiveness, and privilege prior to any disclosure to [plaintiff]").

Ordering imaging of entire computers and other devices—the predicate for such forensic examination—is no small matter because of the vast amount of data they contain. "A mirror image contains all the information in the computer, including embedded, residual, and deleted data. A Court must be mindful of the potential intrusiveness of ordering forensic imaging, however. Before compelling such imaging the court must weigh inherent privacy concerns against its utility." *Wynmoor Cmty. Council*, 280 F.R.D. at 687 (internal citations and quotations omitted). Still, Skyryse recognizes the gravity of Moog's accusations and has agreed to forensic imaging, proposing a structure for the forensic searching that goes far beyond those endorsed by many courts.

Skyryse's proposal would not just allow Moog's counsel and experts to instruct iDS to search the millions of files on Skyryse's machines for potentially discoverable information, but also would provide Moog with detailed information about the data itself, permitting Moog to explore and test its allegations of document destruction and alleged spoliation. This is important, for Moog has repeatedly jumped to the conclusion that any potentially discoverable documents that have been deleted necessarily amounts to spoliation of evidence, though the investigation (including into whether any deleted documents are not recoverable) remains underway. In any event, Skyryse's proposal addresses this. For example, iDS would be required to use industry-standard methods to index the user data on each image (Exh. A, ¶ 1); interrogate the images using

Moog's thousands of search terms from the Moog Filename List and Moog Hash Value List (*id.*, ¶ 3); provide a "red flag report" reflecting iDS's independent judgment about whether any alleged Moog confidential information was "stored on, transferred to, or transferred from" the devices being inspected (*id.*, ¶ 2); and provide "all underlying data relied upon to generate the reports." (*id.*, ¶ 5.) This underlying data would give Moog the forensic information it claims to need, including about whether such files had been deleted or not. iDS would prepare: (1) a list of the contents of each image used to generate the reports with available metadata; (2) a report with all available information about file access; (3) browser history; (4) a list of any deleted files that are recoverable or identified through other techniques; (5) a report of external device connections to the devices and evidence of any file transfers; (6) a report of any forensic countermeasures, such as potential "file scrubbing" or "shredding"; and (7) any other raw forensic data iDS deems is potentially related to the receipt, use, access, or deletion of alleged Moog confidential information. (*Id.*) By any measure, Skyryse's protocol is thorough, reasonable, and robust. And while Skyryse has proposed a protocol that leverages the file names and hash values that Moog has identified so far, the parties are free to meet and confer about reasonable modifications to the list of search terms as the investigation continues.

III. MOOG'S COMPLAINTS ABOUT SKYRYSE'S PROPOSED PROTOCOL ARE UNPERSUASIVE.

Moog criticizes Skyryse's proposal on several grounds, none of which is persuasive. Moog argues that the proposal would erect a "wall" between Moog and the discoverable materials, and complains that the neutral forensic vendor iDS—which Moog selected for its expertise—would be the one to carry out the inspection of the forensic images, while "Moog's retained experts and outside counsel would get no access." (Apr. 19, 2022 Letter from R. Andoh to Court, Dkt. No. 74

at 3.) This is plainly wrong. Moog would not be walled off from the process, nor would its counsel or experts be denied access to the discoverable material.

Moog's counsel (working with its experts) already have formulated and given to Skyryse's counsel lists of literally *tens of thousands of file names and hash values to use as search terms* designed to lead to the discovery of information relevant to Moog's claims that the defendants misappropriated trade secrets.[2] The idea that Moog's counsel and experts would have no input into the forensic search is baseless. And Moog is free to propose additional search terms if it views the tens of thousands it already has offered as deficient. Moreover, the notion that Moog's experts and counsel "would get no access" to Skyryse's discoverable materials is just wrong. As explained above, Skyryse's proposal would give them *direct access* to the discovery materials that result from the search process; those materials will be produced to Moog's counsel after the searches are run and after Skyryse's counsel have reviewed the materials for privilege and responsiveness. Moog's counsel and its experts will be free to examine this discovery material at length, and use it as they see fit to prepare their case. Moog's suggestion that it would lack input into the process or access to the resulting discovery has no merit.

Moog's speculative theories about the alleged misappropriation cannot justify the unbounded forensic discovery it seeks. Moog speculates that "Defendants have stolen over 1.3 million of Moog's files covering a huge array of Moog's intellectual property"—without

[2] These tens of thousands of search terms are in the "Moog Filename List" and "Moog Hash Value List" mentioned on page 3 of Skyryse's proposed forensic protocol. As Skyryse has previously noted to the Court and to Moog, Moog's Filename and Hash Value Lists contain broad swaths of public information, including generic file names readily found in common, commercially available applications. This has created undue burden and delay, because searching for such terms necessarily returns "hits" that correspond to non-Moog files. Skype's proposed forensic protocol therefore uses Moog's lists in searching for potentially responsive information, "as further modified by Moog to remove all files that did not originate with or belong to Moog."

sufficiently identifying specific files that are the alleged trade secrets—and postulates that "the ways in which the data in those files *could have been* misappropriated is *virtually limitless*." (Dkt. No. 74 at 8.) As explained in more detail below, while Moog has claimed that volumes of data were copied, it has yet to identify its own trade secrets with particularity, as it will need to do in this action. But Moog has been able to generate tens of thousands of file names and hash values that purportedly relate to its alleged trade secrets. The most reasonable, efficient, and fair way to proceed is not by letting Moog's lawyers and experts have "open season" to explore the entirety of Skyryse's computers with no restrictions, hoping to create a narrative of what "could have been" misappropriation. It is to have iDS run Moog's own search terms (many thousands of them) that have at least some arguable connection to Moog's alleged trade secrets to conduct a forensic investigation of what actually occurred that is relevant to Moog's claims.

IV. MOOG IS ATTEMPTING TO OBTAIN DISPROPORTIONATE DISCOVERY FAR BROADER THAN THE SCOPE OF ITS ALLEGED TRADE SECRETS.

Moog's attempt to have its own lawyers and experts lead an unbounded forensic investigation into the entirety of Skyryse's computers (and every file in them)—before Moog has even identified its alleged trade secrets with sufficient particularity—is a classic example of over-reach that courts in New York and around the country routinely warn against. In *MSCI Inc. v. Jacob*, for example, the court explained that "the law requires that a trade secret plaintiff identify trade secrets with reasonable particularity early in the case. Only by distinguishing between the general knowledge in their field and their trade secrets, *will the court be capable of setting the parameters of discovery* and will defendants be able to prepare their defense." 36 Misc. 3d 211, 213–14, 945 N.Y.S.2d 863, 865 (N.Y. 2012) (internal citations omitted); *see also Xerox Corp. v. IBM Corp.*, 64 F.R.D. 367, 371 (S.D.N.Y. 1974) ("The burden is upon the plaintiff to specify [its alleged trade secrets], not upon the defendant to guess at what they are .... Clearly until this is done,

neither the court nor the parties can know, with any degree of certainty, whether discovery is relevant or not; and it is doubtful whether [defendant] can undertake a meaningful discovery program ...."); *A&P Tech., Inc. v. Lariviere*, No. 1:17-cv-534, 2017 WL 6606961, at *9 (S.D. Ohio Dec. 27, 2017) (requiring particularized trade secret identification for DTSA claim before discovery where, as here, "[i]t is too early to tell whether Defendants are hiding their misappropriation of Plaintiff's trade secrets or *whether Plaintiff's lawsuit is an attempt to use litigation as a means of discovering the trade secrets of a competitor*.") As these federal and state courts all observed, the need for a plaintiff to identify its trade secrets before embarking on significant discovery is both a matter of fairness to the defendant and a basic requirement for effective discovery and case management. Skyryse's proposal allows Moog to take significant forensic discovery, within reasonable limits.

The *MSCI* court explained precisely the problem posed by Moog's attempt to use its forensics proposal to obtain far-reaching, unlimited discovery. "[I]t would be unfair to allow plaintiffs to discover [defendants'] trade secrets prior to revealing their own. Should defendants remain in the dark as to the explicit portions of the source codes that plaintiffs deem to be trade secrets misappropriated by defendants, plaintiffs, once privy to [defendants'] source codes, could tailor their theory of misappropriation to [defendants'] work." *MSCI*, 36 Misc. 3d at 214, 945 N.Y.S.2d at 866 (precluding plaintiffs "from seeking further discovery from defendants until they identify, with reasonable particularity" their alleged source code trade secrets). Moog's expansive forensic protocol would let it do exactly what courts have long warned against: make accusations that some trade secrets exist and were "stolen," gain access in discovery to Skyryse's proprietary information such as source code and technical documents, and then "tailor their theory of

misappropriation" for litigation purposes to match Skyryse's technology. The Court should not countenance such tactics.

Skyryse reserves its right to seek an order compelling Moog to identify its allegedly misappropriated trade secrets with sufficient particularity. It plainly is not enough for Moog to simply repeat its mantra about "1.3 million files" with little specificity to justify the unfettered discovery it seeks. For present purposes, however, Skyryse has agreed to the Stipulated Order and the need for an effective—and fair—protocol for searching the information delivered to iDS. Only Skyryse's proposal, which uses Moog's own suggested search terms and leverages the independent forensics firm's capabilities, strikes the proper balance.

V. MOOG'S PROPOSED PROTOCOL IS UNPRECEDENTED, EXCESSIVE, AND UNLIMITED.

Moog has been clear that it wants direct, unfettered access to the images of the Skyryse computers—in their entirety and with no restrictions—so its counsel and experts can peruse and examine them unhampered by using search terms relevant to this case, and without the neutral forensics expert's involvement other than some passive monitoring. Moog has said as much, urging the Court to allow Moog's "retained experts and outside counsel to *directly inspect forensic images of the defendant's devices*" including the millions of files on them that have nothing to do with this case. (Dkt. No. 74 at 4.) Moog claims that Skyryse's concerns about this unbounded approach will be sufficiently addressed because (1) Skyryse's counsel can review the images for privileged communications and remove them, and (2) Moog's wide-ranging inspection of the images would be "subject to the protections of the Protective Order." (Dkt. No. 74 at 4-5.)

Moog misses the point. Both sides' proposals allow for privilege review, and both sides of course are bound by the Court's protective order. It does not matter that iDS, rather than Moog's lawyers and experts, would have physical custody of the machines under Moog's proposal, since

their entire contents still would be divulged without restrictions. Nor does it matter that Moog's counsel's and experts' review of the images would be monitored and governed by the confidentiality restrictions of the protective order, for these steps do nothing to prevent a limitless, wide-ranging fishing expedition into irrelevant, sensitive information with no connection to this case.

The unfixable flaw in Moog's proposal is not about preserving privilege or having lawyers comply with confidentiality restrictions. It is that it would unfairly, and with no showing of relevance, need, or proportionality, give Moog's counsel and experts open access to *Skyryse's entire computer systems* rather than to the portions that may actually be relevant to the parties' claims and defenses. Moog's proposal would allow its attorneys and experts to access innumerable files that have nothing to do with this case, that are not responsive to any of Moog's thousands of search terms, that are competitively sensitive and valuable, and that likely contain private and even personal information. Under even the liberal standards for relevance in discovery, Moog cannot make a straight-faced argument that obtaining direct access to *all* the information in a single Skyryse computer (much less several, or potentially dozens) is "relevant to any party's claim or defense or proportional to the needs of the case." Fed. R. Civ. P. 26(b)(1).

Moog has provided the Court with no authority justifying the unprecedented and virtually unlimited forensic discovery it seeks. Moog relies heavily and repeatedly on an unpublished, unreported Special Master's recommendation adopted by the court in *Allergan, Inc. v. Merz Pharmaceuticals, LLC*, No. SACV11-00446 AG, 2011 WL 13323241 (C.D. Cal. June 9, 2011). But that case is distinguishable and inapplicable. First, the dispute did not deal with forensic images of entire computers maintained by a corporate defendant, unlike the Skyryse computers implicated here, much less dozens of them. To the contrary, the dispute concerned "the production

of information stored in electronic media in the possession of the Individual Defendants," "not company equipment," *id.* at *1, and "the media in question" consisted of "hard drives and external storage media." *Id.* at *3. Second, while the Special Master allowed the plaintiff "direct access to the forensic images" of the Individual Defendants, he only did so "subject to the opportunity of the Individual Defendants *to eliminate any material for which a privilege or other objection to production is claimed*." *Id.* at *4. This, after the Special Master acknowledged but expressly declined to rule on the defendants' relevance objections, hoping the parties would avoid "a potential relevance war." *Id.* at *3. By contrast, Moog has not proposed any process by which Skyryse or the other defendants can "eliminate" sensitive, irrelevant non-privileged material before it is made accessible to Moog. Moog wants "to directly inspect" the entirety of the defendants' devices, whether the material is relevant to this suit or not.

Nor is *BalanceCXI, Inc. v. International Consulting and Research Group, LLC*, No. 1:19-CV-0767-RP, 2020 WL 7034123 (W.D. Tex. Nov. 24, 2020), helpful to Moog. There was no dispute over the defendants turning over devices to the plaintiff's counsel for imaging and examination, *because they had stipulated* to such a protocol in view of the unique facts of that case. *Id.*, *1. The dispute was about whether the plaintiff had timely returned some of the defendant's devices after imaging, and whether another could be made available for imaging pursuant to the stipulated order. Nothing about *BalanceCXI* suggests that absent a stipulation the Court should permit Moog unfettered access to an alleged competitor's computer systems in discovery. Moog also invokes *Physicians Interactive v. Lathian Systems., Inc.*, but that case too does not support the sweeping forensic investigation Moog seeks here. No. CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003). Unlike here, the court in *Physicians Interactive* already had found the plaintiff had shown "theft of its trade secrets" (customer lists and source code the

plaintiff had *shown* were trade secrets), entered a preliminary injunction, and ordered discovery including imaging of the defendant's computer equipment that "must be done with the assistance of a computer forensic expert." *Id.*, *10-11. The court never addressed the extent to which the plaintiff's own counsel and experts, rather than an agreed-upon neutral forensic expert, should be permitted to search those images. Nor is *Audio Visual Innovations, Inc. v. Burgdolf*, No. 13-10372, 2014 WL 505565, at *1 (E.D. Mich. Feb. 3, 2014) useful, for in that case the only alleged trade secrets were "information such as customer contact lists," not technologies, and there was no independent or neutral forensics firm involved, much less one the parties had stipulated would image electronic information into which both sides' data may have been intertwined.

VI. MOOG CAN SEEK APPROPRIATE DISCOVERY OF SOURCE CODE AND PROCESS DATA THROUGH OTHER MEASURES.

Moog complains that Skyryse's proposed forensic protocol would be insufficient to permit discovery of "three categories of materials pertaining to the devices": (1) source code and other technical documents; (2) process assets; and (3) forensic data. (Dkt. No. 74 at 9-14.) Moog is wrong on all three counts. These discrete categories of information are best discovered through targeted discovery requests and responses, not through a wide-ranging, unlimited forensic fishing expedition of Skyryse's computers.

A. Source Code and Technical Documents

According to Moog, it needs a forensic protocol that would give its lawyers and counsel unfettered access to Skyryse's "source code and other technical documents" that reside on the computers delivered to iDS. And according to Moog, its own proposed search terms and hash values will not adequately lead it to discover evidence in Skyryse's source code or technical documents if their file names or hash values have changed while in the defendants' possession.

(*Id.* at 9-10.) Moog's argument demonstrates why a forensic examination of entire computers is the wrong vehicle for discovery of "source code and other technical documents."

If Moog believes Skyryse has source code or technical documents that are derived from or incorporate Moog's trade secrets, then it can request Skyryse's source code and technical documents under Rule 34 in discovery. If good cause supports such discovery, then as is customary in modern electronic discovery the parties will arrange for an appropriate, confidential, attorneys'-eyes-only inspection of the relevant source code and technical documents, not a far-reaching exploration of *all* the contents of entire computers, which may or may not contain the potentially relevant and discoverable source code. By contrast, trying to shoehorn discovery of "source code and other technical documents" into a forensic protocol is bound to fail because that effort is both too narrow and too broad. It is too narrow because if Moog has requests for specific source code files that are relevant and discoverable, there is no reason to think they necessarily will be found on the devices in iDS's custody rather than in another source code repository. It is too broad because even if a machine in iDS's custody has discoverable source code that Moog is interested in, this does not justify an expansive and unlimited search of the entire machine and all of its other irrelevant, confidential, private contents.

As the Court is well aware (and as was discussed at the last status conference with Your Honor), litigants in modern intellectual property lawsuits routinely engage in discovery of confidential source code and technical documents using common procedures to safeguard their confidentiality. These include, for example, making the requested, relevant source code available for inspection to counsel and experts on isolated, non-networked machines, at controlled, supervised locations, with restrictions on access, printing, and note-taking. In fact, the Protective Order provisionally entered by the Court acknowledges the potential discovery of "extremely

sensitive" information including "computer code ..., engineering specifications, or other Material" that will be designated "HIGHLY CONFIDENTIAL – SOURCE CODE" and treated with the utmost sensitivity. (Dkt. No. 89, ¶ 1.10.) That same order recognizes that "[t]he parties are discussing protocols pertaining to Source Code and will address these protocols in an addendum to be submitted to the Court." (*Id.*, ¶ 8.1.) This is the norm in cases where highly sensitive source code and technical documents are the subject of discovery, and it does not require or involve forensic inspection of entire computer systems.

Moog thus has suitable means for taking discovery of source code and technical documents, and its desire to obtain such materials is no justification for the wide-ranging, virtually limitless *forensic protocol* it now proposes. In fact, taking separate, targeted discovery of source code and technical documents would avoid the very problem Moog complains about, when it argues that iDS is incapable of taking "a more sophisticated, nuanced approach, executed by someone with experience in aviation software development." (Dkt. No. 74 at 10.) Moog complains that it needs its own expert to "analyze how Skyryse's flight control software is architected," learn "what the relevant source code looks like," and that "iDS does not have the above expertise." (*Id.* at 10-11.) Regardless of whether Moog's criticisms of iDS have any merit, the point is that its counsel and experts "with experience in aviation software development" *can* obtain, review, and consider information pertaining to Skyryse's source code and technical documents when requested through appropriate and customary discovery methods, not through a forensic protocol.

B. Process Assets

Moog makes a similarly misplaced complaint about discovery of "process assets," which it describes as "templates, checklists, tools, test cases, artifacts,[3] etc. pertaining to compliance with FAA regulations." (Dkt. No. 74 at 11 (footnote in original).) Moog claims without evidence that "Skyryse is particularly interested in these extremely valuable process assets" and accuses Skyryse of allegedly "developing a software process using Moog's library of artifacts and other process assets." (*Id.* at 12.) Setting the merits of these accusations aside, they provide no support whatsoever for an unbounded, expansive forensic protocol. As with source code, Moog can seek discovery related to process assets from Skyryse, and its lawyers and experts can then review any responsive information Skyryse produces. Moog's repeated complaint that "iDS does not have the expertise" to search for such "templates, checklists, tools" as part of a forensic investigation thus is misplaced. Moog can seek discovery of process assets separately, and then rely on its own "experts with specific source code and industry experience" to review the produced materials independently of or in conjunction with any forensic work that iDS is doing. (*Id.* at 13.)

Moog's attempts to force this aspect of discovery into the forensic investigation are unavailing. First, it complains defendants are "incapable of or unwilling to" provide discovery related to process assets. (*Id.* at 13.) Not so. The defendants' agreement to the Stipulated Order and ongoing, good-faith discovery efforts show otherwise, and Moog's mischaracterizations of the defendants' state of mind do not justify the expansive forensic investigation it demands. Second, Moog speculates that taking discovery focused on process assets process will "foment[] multiplicative disputes requiring Court intervention" leading to "undue delay." (*Id.*) Skyryse

[3] "An 'artifact' as used here is a completed checklist that proves the company has reviewed the source code at issue and that the code is correct, which would be presented to the FAA in the case of an audit."

disagrees, and is committed to an efficient process, which Moog can facilitate by seeking appropriate and not over-reaching discovery and by promptly identifying its alleged trade secrets with particularity. In any event, Moog's speculation about disputes and delays is unfounded and has nothing to do with whether Moog is entitled to launch an unrestricted fishing expedition into the entirety of Skyryse's computer systems. Third, Moog makes the nebulous assertion that "the full scope of the ways in which Defendants have [allegedly] misappropriated over 1.3 million files—covering a huge swath of Moog's [alleged and unidentified] trade secrets—is unknown to Moog." (*Id.*) But Moog offers no justification for why the forensic protocol Skyryse has proposed, using Moog's own thousands of search terms, combined with suitable other discovery targeted to source code and technical documents, would be insufficient. Moog and its counsel will hardly be "forced to 'guess'" what the facts are as discovery proceeds nor will they be "wearing a proverbial blindfold" as they review and study the results of the forensic investigation and other discovery the defendants provide in response to Moog's requests. (*Id.* at 13.) Moog's hyperbole does not justify drastic, invasive, and virtually unlimited forensic discovery of Skyryse's computer systems, untethered to the claims and defenses in this action.

C. Forensic Data

Moog wrongly suggests that under Skyryse's forensic protocol, it somehow would be denied the ability "to inspect forensic data" regarding the devices in iDS's custody. (Dkt. No. 74 at 14.) Not so. Skyryse has explained above the many ways in which its proposed protocol would ensure that iDS generates and provides to Moog detailed forensic information about the data itself, including about any potential deletion or forensic countermeasures, letting Moog and its experts review that information and test their allegations of document destruction and alleged spoliation. *Supra* at 7-8; *see also* Exh. A, ¶ 5. Notably, Moog does not disparage iDS's expertise, judgment, or abilities in forensic investigation or analysis—indeed, iDS's capabilities in this area presumably

are a reason why Moog recommended them in the first place. Rather, Moog's primary complaint seems to be that using a forensic protocol that lets the neutral forensic expert perform an appropriate forensic analysis "would take too long" and it wants to do it itself. (Dkt. No. 74 at 15.) This, again, is speculation and the prospect of hypothetical delay does not justify giving Moog and its experts unfettered access to Skyryse's entire computer systems.

VII. CONCLUSION

For the foregoing reasons, Skyryse respectfully requests that the Court the proposed order at Exhibit A, adopting Skyryse's proposed forensic protocol.

Dated: May 11, 2022

/s/ Gabriel S. Gross

LATHAM & WATKINS LLP

Douglas E. Lumish (Admitted *Pro Hac Vice*)
Gabriel S. Gross
140 Scott Drive
Menlo Park, California 94025
Telephone: (650) 328-4600
Facsimile: (650) 463-2600
Email: doug.lumish@lw.com
gabe.gross@lw.com

Joseph H. Lee (Admitted *Pro Hac Vice*)
650 Town Center Drive
20th Floor
Costa Mesa, California 92626
Telephone: (714) 540-1235
Facsimile: (714) 755-8290
Email: joseph.lee@lw.com

HARRIS BEACH PLLC
Terrance P. Flynn
726 Exchange Street, Suite 1000
Buffalo, New York 14210
Telephone: (716) 200-5050
Email: tflynn@harrisbeach.com

Counsel for Defendant Skyryse, Inc.